Combining IRAM2 with Cost-Benefit Analysis for Risk Management

Creating a hybrid method with traditional and economic aspects

Dorna Dehkhoda

Information Security, master's level (120 credits)
2018

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
Abstract

The aim of this thesis is to contribute to the risk methodology field by introducing a method that covers both economic and information security aspects. The aim is to provide a way for practitioners to get results that is enough for decision makers to make valid and well-grounded decisions. There are a lot of traditional risk assessment methods that focus on information security. There are also CBA (Cost-Benefit Analysis) methods that are used to make sure investments are cost-effective and provide value for the organization. The aim of this thesis is to combine those and see if they can be merged to one risk assessment method to increase the value of the result. CBA will be added to a more traditional risk assessment method called IRAM2. The thesis will evaluate if they are suited to be used together and if it provides a more valuable result when combining them than only using one of them. The research method that has been used in this study is ADR. It has been used as a way of working when producing a new hybrid method together with some design principles regarding how to combine traditional risk management with economic equations.

Keywords

Risk management, Cost-Benefit Analysis (CBA), IRAM2, SEB Kort, cost-effective risk management, Information security, risk assessment, risk mitigation, economic risk management, risk management implementation, design principles, mathematic equations.
Acknowledgement

I would first like to thank my thesis advisor professor Tero Päivärinta. His guidance has been very helpful and he was always willing to help when I had difficulties with the thesis work and guided me in the right direction.

I would also like to thank my colleagues and managers for being a part of my work and helping me in every step of the way. They have been open-minded and given me time to work with the thesis in any way I needed. They have guided me and agreed to be interviewed and given of their time and energy to help me through the implementation and discussion. Without their participation and input this work would not have been successful.

I would like to especially acknowledge my colleague Marcus Johansson who has given me invaluable help with the CBA equations. This accomplishment would not have been possible without him.

Finally, I must express my gratitude to my family and boyfriend for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. Thank you.

Dorna Dehkhoda
# Table of Contents

Abstract .............................................................................................................................. 1

Keywords ............................................................................................................................ 1

Acknowledgement .............................................................................................................. 2

List of Abbreviations ........................................................................................................... 6

Introduction .......................................................................................................................... 8

Research problem ............................................................................................................... 8

Problem at SEB Kort ......................................................................................................... 9

Knowledge gap .................................................................................................................... 10

Research concept and question .......................................................................................... 10

Purpose ................................................................................................................................ 13

Background .......................................................................................................................... 13

Information Security .......................................................................................................... 13

Risk management ................................................................................................................. 14

Economic aspects of Risk Management .................................................................................. 15

Mitigating risks ..................................................................................................................... 16

Challenges with adopting a Risk Management method ......................................................... 17

Literature review process .................................................................................................... 17

SEB organization .................................................................................................................. 18

SEB Kort ................................................................................................................................ 18

Risk management methods .................................................................................................. 21

Information Risk Assessment Methodology (IRAM2) ............................................................ 21

Cost-Benefit Analysis (CBA) ............................................................................................... 26

Comparing security measures .............................................................................................. 34

Research method .................................................................................................................... 36
**Table of Figures**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Organizational chart of SEB</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>Organizational chart of Corporate &amp; Private Customers</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Organizational chart of SEB Kort</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>The IRAM2 method</td>
<td>22</td>
</tr>
<tr>
<td>5</td>
<td>Coat hanger model</td>
<td>39</td>
</tr>
<tr>
<td>6</td>
<td>View of information flow being assessed</td>
<td>45</td>
</tr>
<tr>
<td>7</td>
<td>New flow introduced</td>
<td>46</td>
</tr>
<tr>
<td>8</td>
<td>Profiling environment part 1</td>
<td>48</td>
</tr>
<tr>
<td>9</td>
<td>Profiling environment part 2</td>
<td>48</td>
</tr>
<tr>
<td>10</td>
<td>Scope of the assessment</td>
<td>50</td>
</tr>
<tr>
<td>11</td>
<td>BIA Confidentiality</td>
<td>51</td>
</tr>
<tr>
<td>12</td>
<td>BIA Integrity</td>
<td>52</td>
</tr>
<tr>
<td>13</td>
<td>BIA Availability</td>
<td>53</td>
</tr>
<tr>
<td>14</td>
<td>Threat profiles that were included</td>
<td>54</td>
</tr>
<tr>
<td>15</td>
<td>Threat profiles that were excluded</td>
<td>55</td>
</tr>
<tr>
<td>16</td>
<td>Example of control effectiveness</td>
<td>56</td>
</tr>
<tr>
<td>17</td>
<td>Example of control strength</td>
<td>57</td>
</tr>
<tr>
<td>18</td>
<td>Columns in risk evaluation</td>
<td>57</td>
</tr>
<tr>
<td>19</td>
<td>Columns in risk treatment</td>
<td>58</td>
</tr>
<tr>
<td>20</td>
<td>Suggested hybrid method</td>
<td>71</td>
</tr>
</tbody>
</table>
## List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBA</td>
<td>Cost Benefit Analysis</td>
</tr>
<tr>
<td>IRAM</td>
<td>Information Risk Assessment Methodology</td>
</tr>
<tr>
<td>IRR</td>
<td>Internal Return Rate</td>
</tr>
<tr>
<td>NPV</td>
<td>Net Present Value</td>
</tr>
<tr>
<td>ROI</td>
<td>Return of Investment</td>
</tr>
<tr>
<td>ADR</td>
<td>Action Design Research</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>SEB</td>
<td>Skandinaviska Enskilda Banken</td>
</tr>
<tr>
<td>ISF</td>
<td>Information Security Forum</td>
</tr>
<tr>
<td>ISD</td>
<td>Information systems development</td>
</tr>
<tr>
<td>TS</td>
<td>Threat strength</td>
</tr>
<tr>
<td>LOI</td>
<td>Likelihood of initiation</td>
</tr>
<tr>
<td>LOS</td>
<td>Likelihood of success</td>
</tr>
<tr>
<td>ALE</td>
<td>Annualized loss expectancy</td>
</tr>
<tr>
<td>SLE</td>
<td>Single loss expectancy</td>
</tr>
<tr>
<td>ARO</td>
<td>Annualized rate of occurrence</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
</tbody>
</table>
Introduction

“Although companies consider security as one of the most important issues on their agenda, many companies are not aware how much they spend on security and if their investments in security are effective.” [19, page 1]

The risk management process is becoming more and more important for organizations, because organizations are becoming increasingly dependent on their information systems and internet services. Because of these dependencies, an attack can have severe consequences for organizations. It can result in heavy losses in data and income, and can also damage the company’s reputation and brand. The risks can occur due to technical failures, system vulnerabilities, human failures, fraud or external events [5]. The risk management process allows decision makers to balance the costs of security measures and gain in capability by protecting the organizations data and IT systems [6].

Research problem

A survey done by Computer Security Institute (2011: 22) and the Federal Bureau of Investigation (FBI) shows that information security costs companies billions of dollars, and it is also costing the economy those amounts. Today, a big question for these companies and governments is how much security is needed and how much money to spend on it. For information security people, it is hard to convince managers to spend money on information security. Managers know that no product can guarantee 100% security and there will still be risks left. The problem here is that the managers and decision makers among other things don’t have access to structured cost-benefit analysis methods to be able to evaluate and compare different solutions [3].

There is a knowledge gap in previous research about cost-benefit analysis within risk management in regards to information security. Many risk management methods do not include those aspects and there is not a lot of experience in research about implementing a cost-benefit risk analysis to mitigate information security risks.
There has been research in CBA in information security but they have been very specific such as doing an analysis on intrusion detection systems or enterprise systems. They are not generic enough to present a framework for information security investments [20]

**Problem at SEB Kort**

“How much security we have versus how much insecurity we have is what management needs to decide upon when weighing up the pros and cons, the costs and the benefits, the risks and impacts of investing in information security.” [16, page 23]

Since SEB and SEB Kort haven’t started using the method they have chosen to get an overview of their risks, this is a problem for them. They don’t have a unified way of managing information security risks and they don’t have a method that employees are aware of and know that they should use when making significant changes.

To understand the situation with risk management at SEB Kort, the CISO has been interviewed. The CISO mentioned that they lack a unified way of working with risk management. SEB has decided that the unified way of working with information security risks in the organization should be with IRAM2 (information risk assessment methodology 2) which is a risk assessment method. SEB Kort has however not yet started implementing the method which they consider to be a problem for them. Currently at SEB Kort, there is no standard for doing risk management, and the quality and depth of the results differ depending on who performs the risk management and what method they choose (if any). The lack of a unified way of working with risk management also creates difficulties in communicating with management regarding investments. Getting started and implementing IRAM2 in practice at SEB Kort would help them with that problem. Since there have been problems adopting IRAM2, making the risk assessment process easier through simplifying IRAM2 is one of the things that will be taken into consideration when creating a new method.

At SEB Kort, the people responsible for risk management have wanted to start working in a unified way with risks for a long time. The work has stopped on a theoretical level and they
have asked for help to start implementing what they have discussed in theory. There are not a lot of resources at SEB Kort that have the time and possibility to make a big effort in implementing a risk management method in practice. To conclude, there are two problem areas at SEB Kort, the first problem being that there are difficulties implementing information security risk management methods in practice. This is due to lack of prioritization and resources but also that there is no unified way of working with risk management. The other problem that follows the first problem is that due to the lack of standardized risk management work, there is no standardized analysis on how to make cost-effective decisions on mitigation.

**Knowledge gap**

After following the process mentioned earlier, the conclusion is that there is a knowledge gap when it comes to combining a CBA method with a more traditional comprehensive risk management method. No such research has been found during the literature review. Finding that kind of combination was the main focus of the literature review process besides giving background information to the subjects discussed. The research that focuses on economic aspects of information security is rather sparse. The work that does exist in the topic does not provide much guidance on how to actually derive how much to invest on security [34].

**Research concept and question**

My intention with this thesis is to use two methods that are used for risk management in different ways and to make a hybrid version of the two methods. I will then implement it at a company called SEB Kort. After the implementation, I will evaluate my hybrid method and state what went well and what needs improvement.

The questions that I will try to answer with my research are:

*What would the benefits be from introducing CBA to a more traditional risk management method?*

And

*How will a hybrid risk management method with IRAM 2 and CBA combined work in a financial Institution?*
“Organizations must consider the economic feasibility of implementing security controls and safeguards. While a number of alternatives for solving a problem might exist, they may not all have the same economic feasibility” [32]. This quote also states as my hypothesis that counting the economic feasibility of a security control should be an important aspect when choosing what to invest in. Another expected advantage from introducing CBA to traditional risk management is that it provides decision support for management and creates arguments in terms that they understand without being experts in information security. Management are often lacking knowledge in computer security but they understand risk and cost-benefit analysis [33].

There has been a shift in risk mitigation and what is technically possible is no longer the most important aspect. The focus has shifted to what is cost-effective and optimal financially. There are many examples where the economic considerations of security are more important than the technical considerations [10]. I have analyzed risk management methods with these considerations in mind and stated that the risk management methods that are used today usually don’t include what according to some is the most important aspect of all. This is the reason that an attempt is made in this study to add that important aspect to a traditional method that lacks it. According to Schneier et al (2005:10) many security systems fail due to misplaced incentives and not for technical reasons as one could assume.

Inducing fear, uncertainty, and doubt is a strategy has been used historically to sell security investments. The strategy is about trying to scare people into investing in security measures and making decisions based on emotions. This might be successful in receiving an initial investment but in the long-run, it won’t be sufficient. There are many different security technologies that are available to solve security issues and vulnerabilities. This creates a need for a more rational methodology to analyze the security investments and make better decisions [35]. The first research questions also aims at evaluating whether communication with management for security investments will become more efficient and if that could be a benefit from combining the two approaches. Reducing risks by investing in security measures that are aimed at reducing the probability of an incident or mitigating the consequences is primary risk management.
strategy. Despite that, the investments in security measure are not very high. One reason for that might be that there is a lack of methods that can help organizations with decision making about how much to spend and what the optimal security measure is. Most organizations also still see security investments as pure costs rather than as an investment [17]. This is where CBA becomes valuable.

In order to avoid costs and risks of security breaches, there needs to be an economic evaluation regarding security investments [37]. The purpose of any investment is to generate return and the return in security investments will in this case be calculated through CBA. The benefits or returns from the investments should justify the costs in terms of enabling business [37]. A key factor when it comes to actually getting value form security is to make sure that the security investments are aimed at protecting the right assets [37]. That is why the traditional risk management method needs to be used as well. It is used to identify the assets and vulnerabilities related to those assets.

My intention with this thesis is to use two methods that are used for risk management in different ways and to make a hybrid version of the two methods. I will then implement it at a company called SEB Kort. To get a practical evaluation of the method that is created, there needs to be a practical implementation. After the implementation, I will evaluate my hybrid method and state what went well and what needs improvement. The first question is aimed at contributing to fill the knowledge gap about CBA used together with traditional risk management techniques. A common view among researchers is that the economic perspectives are becoming increasingly important but the traditional risk management methods lack that perspective and this is an attempt and contributing to adding those perspectives. The second question is added to provide a practical implementation and get a way of evaluating the approach that is presented where economic and technical aspects are combined. Even though the method seems good in theory, implementing it in a real organization will show the practical advantages and disadvantages of using the method. Hackers are known for attacking IT systems that are vulnerable and don’t have the appropriate controls. Another target is well-protected systems as a challenge [35]. Cyber threats that are aimed at important financial institutions
create a special universe of concerns. The number of breaches that threaten or try to interrupt their services are shocking. For financial institutions, the risk management concerns are particularly dangerous [36]. This is a reason that it is relevant to try this method in an organization where risk management is essential.

**Purpose**

For an organization to be able to accomplish its goals, whatever it might be, the organization need to have secure IT systems that store, process or transmit information. To be able to do that, managers need to be able to make well-informed risk management decisions [6]. Having structured methods to analyze, measure and reduce risks in a cost effective way, is a way of achieving that. The purpose of this research is to combine a structured method to define, analyze and measure risks with a structured method for cost effective mitigation. It is also to fill the knowledge gap regarding the combination of traditional risk management methods with methods that calculate financial benefits. The goal is to produce a method that can be used to identify and analyze risks and vulnerabilities that also shows what mitigation is financially beneficial. The method should have both of those aspects as a result of one cohesive process.

**Background**

This chapter describes the background of information security and risk management and also gives explanation to the organization where the study will be conducted.

**Information Security**

Information security is about protecting valuable information, and it is a concept that has been around for a very long time. Today, information security can be explained by four key aspects; availability, integrity, authenticity and confidentiality. Availability means that information should be available for authorized people then it’s needed. Integrity refers to ensuring that information has not been modified by someone unauthorized. Authenticity means validity and genuineness of information. Confidentiality is about protecting information from being disclosed to someone unauthorized [15].
Nowadays, there is more a focus on managing information security rather than just IT security. Earlier, the focus was mainly on IT security and the people working with those issues were IT and technical experts. Things started to shift in the early 90’s towards expanding from just IT security to also include security in regards to people, processes and information. This is an area than has continued to develop to where we are today [16].

**Risk management**

Webster’s dictionary defines risk as “exposure to loss” [4]. In a business perspective, risk is the possibility of an event which would reduce the value of the business if the risk would occur [13]. The view on risk management that will be the base of this research is defined by Stoneburner et al., (2002: 6) is the following:

> “Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization’s information assets, and therefore its mission, from IT-related risk.” [6, page 1]

> “An effective risk management process is an important component of a successful IT security program. The principal goal of an organization’s risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.” [6, page 1]

Risk management can also be defined as the overall process that integrates the identification and analysis of risks to which an organization is exposed. It also provides an assessment of the potential impact on the business and enables a decision about which action to take to mitigate risk to an acceptable level or eliminate it if possible [11]. Risk management can be used to answer questions like: “which security level is good enough?” “How much resources should be spent to mitigate each risk?” [5] Risk management in general is an area that has been a subject to research extensively and there are many different models for the purpose [12].
The information security risk management usually contains the following steps [17]:

1. Identifying business assets
2. Identifying threats and assessing damage that can be caused if attacks would occur
3. Assessing vulnerabilities
4. Assessing risks
5. Implementing security measures to mitigate risks
6. Monitoring effectiveness of security measures

There have been great advancements in security technology in the past years but the security level has not improved as much, which can be considered the reason as a main reason for information security risk management getting more attention.

According to Alberts and Dorofee (2002: 18) a comprehensive risk management approach should contain the following:

- assets, threats and vulnerabilities
- enables decision-makers to prioritize based on what is important to the organization
- organizational issues related to how people use the computing infrastructure to meet the business objectives of the organization
- technological issues related to the configuration of the computing infrastructure
- should be a flexible method that can be uniquely tailored to each organization

**Economic aspects of Risk Management**

“When we discuss information security, we must look at not only technology issues but also economic incentives.” [20, page 43]

For the past decade, researches have started to realize that information security is not only a problem that is solved by technical solutions, they have started to also include an economical aspect to information security. Security measures are financial investments and they need to be presented through economic gains and losses instead of just a technical analysis. [17]
“Every risk has a cost and that cost can be (more or less precisely) quantified [13].” Earlier, organizations always looked for technical solutions to prevent threats, but for the past years, researchers have realized that information security can’t be solved with only technical solutions. They have seen the need for economic aspects and have started to include those. The benefits of this are that the measures can be more cost-effective and the decision makers can understand their security investments better. The implications of security failures are replaced by an analysis of economic losses of that failure [9]. In the recent years, there has been a shift in focus regarding mitigating risks from what is technically possible to what is cost-effective and optimal from an economic aspect [10].

The main goals with risk management is to enable organizations to fulfill their mission by securing their IT systems and enabling management to make decisions on placing resources on security measures and being well-informed to be able to make enhanced decisions [6]. Risk management is a crucial element for ensuring long-term business success because it provides an effective approach for measuring the security through the identification and valuation of assets, threats, and vulnerabilities and offers methods for the risk assessment, risk mitigation and evaluation“[19].

**Mitigating risks**

The strategies for risk mitigation in information security can be divided into 4 categories [17]:

- Avoiding risks
- Reducing risks
- Transferring risks
- Accepting risks

Avoiding risks means that the organization eliminates the source of the risk or the asset’s exposure to the risk. Reducing risks means implementing security measures or policies to reduce the asset’s exposure to the risk. Transferring risks means transferring the responsibility by for example outsourcing or buying insurance. Accepting risks means that you accept possible
losses as a cost of doing business. This can be used when the cost of mitigating a risk is greater than the total losses.

**Challenges with adopting a Risk Management method**

At SEB Kort we have experienced that the time and effort that risk management takes is a problem. Like in many other organizations, focus is on income driven innovative projects. Risk management can be an administrative overburden that the organization doesn’t have time for. A result is that the risk often is deprioritized.

For a risk manager to become successful he or she needs the support of the organization and that is why a clear and well developed method is necessary. Risk management needs to be a systematic process that is applied in a disciplined manner [26]. To get this support and understanding from the organization, the method needs to be standardized and easy to communicate to the rest of the organization including managers. To get the support needed, there needs to be consensus regarding the process that is not dependent on who currently is risk manager. The purpose and results can also be communicated better if the risk management is done properly.

**Literature review process**

The search engine used for literature review has been Google scholar and Scopus. The search terms have mainly been the following: risk, information security, risk assessment, risk methodology, risk management, financial risk management, economic incentives for risk management, CBA, IRAM2, CBA risk assessment, CBA information security, cost effective risk management, risk mitigation, combining risk management with CBA. These types of sources have been searched through: books, articles, abstracts, dissertations, theses, research reports and websites.

When going through the result in the search engines, some material could be excluded based on title only. If the title showed a completely different subject than this study, they were not studied in more detail. The material that seemed to be about the right subject was first skimmed through. The next step was to read the abstract and if still relevant, save it in a list of
articles to read. Those articles were categorized based on the subject they were discussing. The categories were risk management, information security, CBA, IRAM2, mathematic, general research methods and other. The articles were reviewed in detail later. The original sources were also read and in some articles, the references pointed to other interesting articles that were also read.

The structure, general reasoning and main ideas were identified. Some key elements and ideas that are related to my subject have been referred to and discussed. Some of the key elements that were analyzed were: problem, purpose, research question, data gathered, findings, conclusions and recommendations for further studies. When I concluded that I had gathered enough material, I started to write down the patterns and themes that were found in several of the studies. I identified connections and common viewpoints that created the concepts in my literature review. From that I created headings in my own study where I described and discussed those theories that have been found. One example is that I found the theory about needing to include financial perspectives in risk management in several studies. I made connections between different studies that were built on that theory and saw a pattern. I started to build my own work based on that theory and develop that theory further.

**SEB organization**

SEB is a Scandinavian bank and financial group with its headquarters in Stockholm. It is a bank that has corporate customers, private customers and institutions. Their main business area is banking but they also have services in the insurance industry. It is a bank that was formed in 1972 through a merger between Skandinaviska Banken (established 1864) and Stockholms Enskilda Bank (Established in 1856). They also acquired the Swedish insurance company Trygg-hansa in 1997 [14].

**SEB Kort**

SEB Kort is a subsidiary to SEB, the company is fully owned by SEB. SEB Kort was established the year 1999 and has its headquarters in Stockholm. Organizationally it is placed under Corporate & Private Customers. It is a Scandinavian financial company that is one of the leading card issuers in the Nordics. SEB Kort has around 650 employees divided in Stockholm,
Oslo, Copenhagen and Helsinki. The focus of SEB Kort is card and card-related services, payments and travel administration. Their customers are both private and corporate customers. It is a company that has a lot of IT systems and a big IT staff. They have a big focus in digitalization which means that there are a lot of development projects that the IT department handles. Their main focus is on corporate customers and developing new corporate payment solutions. They have travel account solutions for corporations and also issue cards. They issue cards with their own brands such as SEB and Eurocard, but are also the issuer for many co-brand cards such as Circle K, SAS Eurobonus and Nordic choice club Mastercard. The new digitization era has also led to new services such as digital wallets and digital receipts.

Figure 1, Organizational chart of SEB
Figure 2, Organizational chart of Corporate & Private Customers

Figure 3, Organizational chart of SEB Kort
Risk management methods
In this chapter, the two methods that will be used in this study are presented.

Information Risk Assessment Methodology (IRAM2)
IRAM2 is an end-to-end risk management methodology developed by the ISF (Information Security Forum). IRAM2 is a method that has a business perspective and includes different aspects. The method is developed and renewed to meet new challenges within risk management. The method has six key objectives that describe how the method can be helpful for organizations [8]:

- A simple, practical and rigorous approach: there is a focus on simplicity throughout the implementation but it is still a rigorous method that enables a deep analysis that can be helpful in making strategic business decisions

- Unified understanding: a common framework and vocabulary is helpful for risk assessors and management to understand each other and have the same understanding

- Business perspective: the risks are assessed from a business perspective and the result should be in business terms.

- Focus on significant risks: The method allows for identifying the most significant risks so that management can decide where to focus the resources.

- Engage with stakeholders: The method provides an organised way to engage between risk practitioners and other stakeholders.

In many organizations, digital information is becoming extensively important and is at the core of their business. To use the digital information in a valuable and effective way is key to having a successful business. The other perspective is that new digital technologies result in new risks and the impact of these risks are growing. This results in the need for organizations to focus more on managing their risks. IRAM2 is an end-to-end approach designed to meet those challenges with a business perspective on risk management.
Phase A: Scoping
The first phase in IRAM2 is about developing an environmental profile and defining the scope of the assessment. The risk manager is supposed to develop an understanding about the organization as a whole and more specifically about the environment or process to be assessed. In IRAM2, an environment is the people, processes, technology and pre-existing conditions within the scope of the assessment. The scope should also be defined and agreed upon together with the stakeholders. Understanding the environment is called profiling in IRAM2 terms, and the environment should be separated into components (business service, business process and
technology service). In the scoping step, it should be determined which business services, business processes and technology services should be in scope. It should also be defined which parties should be involved in the risk assessment.

The steps that should be performed in this phase are:

1. Develop a profile of the environment
2. Develop the scope for the assessment

**Phase B: Business Impact Assessment**

The purpose of this phase is identifying the information assets and to assess the potential business impact if information assets are compromised. The conclusion of the BIA will help the organization get a solid understanding of the information assets in the environment being assessed and their business impact ratings. The realistic and worst case business impacts should be rated. The impacts are assessed through confidentiality, integrity and availability perspectives. The business impacts should be assessed without any security controls taken into consideration since they will be processed in later steps.

The steps in this phase are:

1. Identify the information assets
2. Assess business impact

**Phase C: Threat Profiling**

This phase is about profiling and prioritizing all the threats that are relevant to the environment that is being assessed. In IRAM2, a threat is identified as “Anything that is capable, by its action or inaction, of causing harm to an information asset”. All the relevant threats should be profiled and prioritized. Then, the potential ways that the highest priority threats could harm the environment should be identified. The threats are grouped into three categories; adversarial, accidental and environmental. The threat landscape does not need to be done for each IRAM2 assessment, and can be seen as a threat landscape for the organization as
a whole. Threat profiling (step 2) is about modeling the behavior of threats, which is done by assessing threat attributes. Those attributes are capability, commitment, competence, culture, history, intent, motivation, origin, predisposition, privilege and severity. This results in two risk factors; likelihood of initiation (Loi) and threat strength (TS). Loi and TS is derived for each threat group. The prioritizations of threats are based on Loi and TS. Then the threat events that are associated with each threat are identified. A threat event is “An action (or lack thereof), initiated by a threat against an asset, which is capable of causing harm” [8]. The final step is to identify which information assets that the threat event could impact. In conclusion, this phase should result in an understanding of the in scope threats, the related threat events and how they can affect information assets.

The steps included are:

1. Populate the threat landscape
2. Profile threats
3. Produce a prioritized threat landscape
4. Scope and map the threat events
5. Identify and map the information assets impacted by each threat event

**Phase D: Vulnerability Assessment**

Vulnerability is a weakness in people, process or technology in an environment, which could be exploited by one or more threats [8]. This phase is about identifying the vulnerabilities that are associated with each threat event that is in-scope for the environment being assessed. There should also be an assessment of the degree of vulnerability of each component in the environment being assessed to the in-scope threat events. The security controls are mapped to each threat event to determine the degree of vulnerability. In IRAM2, the vulnerabilities are assessed by assessing the effectiveness of corresponding controls. Then assessing a control design effectiveness and operational effectiveness is considered. The main focus should be on design effectiveness. Control strength is a subjective assessment of the aggregate effectiveness (or
lack thereof) of all the controls mapped to a specific combination of threat event and component [8].

The steps in this phase are:

1. Identify vulnerabilities and related controls
2. Assess the effectiveness of identified controls
3. Determine the control strength for each combination of threat event and component

**Phase E: Risk Evaluation**

The objective is to evaluate the remaining risk factors and the derivation of the residual risk rating for each risk. The output of this phase should be a prioritized residual risk profile. The first risk factor (step 1) derived is Likelihood of success (Los), The likelihood that the strength of a threat will be sufficient to overwhelm the strength of controls in place resulting in a successful threat event [8]. Step 2, deriving the residual likelihood of each risk takes both Loi and Los into account. In step 3, the residual impact rating should be determined, which is the business impact rating after the relevant impact scenario has been determined and the effect of the controls in place has been assessed [8]. The final step is to derive the residual risk rating which is accomplished by plotting residual likelihood and residual business impact on a risk matrix for each risk. The risks can then be prioritized based on their residual risk rating.

The steps are:

1. Derive the likelihood of success
2. Derive the residual likelihood
3. Determine the residual business impact rating
4. Derive the residual risk rating
Phase F: Risk Treatment

The last phase is about determining a risk treatment approach for each identified risk and creating a risk treatment plan. It should be determined in this phase whether each risk exceeds the organization’s risk appetite. An organization’s risk appetite defines the amount of risk that they are willing to accept to achieve their objectives [8]. To which category the risk belongs to is determined in this phase. The risk categories are financial, reputational, customer and health and safety. That should be compared to the organization’s appetite in each relevant risk category.

The steps of the final phase are:

1. Evaluate each risk against the risk appetite
2. Create a risk treatment plan
3. Execute the risk treatment plan and validate results

Cost-Benefit Analysis (CBA)

With all security measures, there is a limit to how much resources companies and people in general are willing to spend. The limit depends on the value of what is being protected and how much reduced cost of losses will be gained by implementing the security measure. CBA can be used to make this evaluation. There are different views on CBA in risk assessment. One view is that CBA can be used to do a trade-off between the cost of implementing a security measure and the risk level. The purpose will then be to get the best security level possible in regards to the economic limits that have been set in the evaluation. The second view is that CBA is used to weigh cost of implementation against the benefits that will be gained from the security measure. The purpose is then to have a tool to help companies and organizations choose cost-effective security measures. With this method, it is possible to estimate the optimal amount of money to spend on security measures to protect a certain asset [1]. In this paper, the second view of CBA is the one that will be used. The reason that the second method is used in this paper is because the purpose is to get more insight to whether an investment is economically feasible or not. The second view helps solve the problem of being able to communicate with
management about the economic feasibility of the investment that is proposed which is what SEB Kort wishes to accomplish.

Generally, cost-benefit analysis in information security can be done the following way [2]: The first step is to assign values to the information assets within the company. If it is a hardware asset, the value can be based on the cost to replace the hardware. If it is software, the value can be measured by measuring the cost of recreating or recovering the asset or the data lost. The second step is to estimate the potential loss for each risk. The next step is to estimate the like likelihood of each risk. The loss in case of an attack should be an upper bound to how much an organization should spend on security measures. Put simply, the cost for a security measure should never be more than the potential loss. The likelihood of an attack happening should also be considered when estimating how much is cost-effective to spend on a security measure. With all this information, organizations can make rational and efficient choices.

CBA (Cost-Benefit Analysis) has gained popularity in recent years and what was new with CBA was that it didn’t only calculate loss but also both the costs and the benefit of the security measure [20]. To be able to make a cost-effective and correct decision, the organization needs to know the risks of each asset, the value of each asset and the cost of protecting it. IRAM2 in combination with a CBA-analysis will include all of those aspects. The IRAM2 method will be used in the beginning to scope and identify which steps should be moved forward into the CBA analysis phase. The result of the CBA analysis will be used later in the IRAM2 where it is suited. Where it suits best will be decided during the implementation, possibly phase E. The methods will complete each other since IRAM2 is needed to scope and identify risks to calculate on and CBA is needed to calculate and give values and estimations that can be used in the IRAM2 process.

In this thesis CBA analysis will be used to calculate the costs and benefits for mitigating significant risks. The way that the CBA analysis will be done is the way that Bojanc et al (2013:5) have described it in their article. What needs to be calculated in the CBA analysis as they described it is:
• The probability of a security incident occurring (contains estimated values of the vulnerability and the threat probability)

• The financial loss due to a security incident (contains estimated values of cost of equipment replacement, cost of repairs, income loss, productivity loss, loss due to non-compliance and indirect losses)

• Which risk treatment to choose (reduction, transfer, avoidance or acceptance). That is measured by considering the probability of an incident occurring and the financial loss due to that incident, and that is compared to these estimated values:
  - maximum risk value that is still acceptable for the organization
  - maximum one-time loss that is still acceptable for the organization
  - minimum risk value that is still meaningful for the organization

• What security measure to choose (preventive, corrective, detective). The security measures are weighed against each other by calculating the security measure productivity and the cost of the security measure.

• The benefit of the security measure (can be calculated through ROI, NPV or IRR)

**Chosen CBA implementation**

The chosen CBA method is developed Bojanc et al (2013:5). This is a simplified description of the equations. Further details about the equations can be found in their article.

*Equations 1-8 are about identification and evaluation of the threats and vulnerabilities.*

*Equation 1 (Probability of a security incident occurring)*

\[ \rho = T \cdot v \]

This equation calculates the probability of a security incident occurring and gives a value between 0 and 1. \( \rho \) is the product of the threat probability (\( T \)) and the asset vulnerability (\( v \)).
Equation 2 (Financial loss due to a security incident)

\[ L = L_s + L_r(t) + L_i(t) + L_p(t) + L_{SLA} + L_{indirect} \]

Equation 2 calculates the financial loss due to a security incident which \( L \) represents. The total financial loss is dependent on these variables:

- \( L_s \) is the cost of equipment replacement
- \( L_r(t) \) is the price of repairs paid to employees or external contractors to eliminate the consequences if the security incident and restore the system.
- \( L_i(t) \) is the corporate income loss on the revenue side due to a system or service failure as a result of the incident.
- \( L_p(t) \) is the organization productivity loss due to an incident.
- \( L_{SLA} \) is the loss due to non-compliance with statutory provisions or contractual obligations.
- \( L_{indirect} \) are the indirect losses with potential long-term consequences like damage to reputation, interruption of business processes, legal liabilities and loss of intellectual property.

Equation 3 (Cost of repairs)

\[ L_r(t) = n \cdot p \cdot t_r \]

The cost of repairs is calculated by multiplying \( n, p \) and \( t_r \). \( n \) represents the number of employees working to fix the problem. \( p \) is the average wage of those employees. \( t_r \) is the time required to repair the problem.

Equation 4 (Corporate income loss)

\[ L_i(t) = EF_i \cdot i \cdot (t_r + t_d) \]

The corporate income loss is calculated by multiplying the following:
EF is the reduction of income due to the incident (value between 0 and 1)

The variable i is the average income per time unit.

t is the time required to repair the problem + t\text{d} is the time required to detect the incident.

**Equation 5 (Productivity loss)**

\[ L_p(t) = m \cdot EF_p \cdot i \cdot (t_r + t_d) \]

\(L_p(t)\) is the productivity loss which is calculated by multiplying the following:

m is the number of employees with limited productivity

\(EF_p\) represents the reduction of productivity due to the incident (value between 0 and 1)

\(i\) represents the average wage of the employees with limited productivity

\(t_r\) is the time required to repair the problem + \(t_d\) is the time required to detect the incident.

**Equation 6 (Financial loss similar to equation 2)**

\[ L = L_s + n \cdot p \cdot t_r + EF_i \cdot i \cdot (t_r + t_d) + m \cdot EF_p \cdot i \cdot (t_r + t_d) \]

\[ + L_{\text{SLA}} + L_{\text{indirect}} = (n \cdot p + EF_i \cdot i + m \cdot EF_p \cdot i) \cdot t_r + (EF_i \cdot i + m \cdot EF_p \cdot i) \cdot t_d + L_s + L_{\text{SLA}} + L_{\text{indirect}} \]

Equation 6 is a detailed view of equation 2-5. The difference is that here, the factors from equation 2 are grouped by their time dependency.

**Equation 7 (Financial loss in monetary units)**

\[ L = L_1 + t_r + L_2 + t_d + L_3 \]

Equation 7 is another simplified representation of equations 2-5.
Equation 8 (Security risk)

\[ R = \rho \cdot L = T \cdot v \cdot [L_1 \cdot t_r + L_2 \cdot t_d + L_3] \]

Equation 8 is a representation of equations 1-5. Here, the probability of a threat incident is added to equations 2-5. \( R \) is the total security risk.

Equations 9-13 is about selecting the appropriate risk treatment.

Equation 9 (Security breach probability)

\[ \rho(T, v; C_p) = T \cdot v^{\alpha_p C_p + 1} \]

\( p \) is the security breach probability, \( T \) is attack probability, \( v \) is vulnerability and \( C_p \) is the cost of preventive security measures. The second \( T \) is multiplied with \( v^{\alpha_p C_p} \) which is the vulnerability value with the preventive security measure in place. These multiplied give us the probability of a security breach.

Equation 10 (Time to repair)

\[ t_r = t_r^0 e^{-\alpha C_c} \]

\( T_r \) is the time to repair. \( t_r^0 \) is the time needed to repair without the implementation of a security measure. \( e \) is a mathematic variable with the value 2.71. \( \alpha C_c \) is investing in a corrective security measure.

Equation 11 (Time to detect)

\[ t_d = t_d^0 e^{-\alpha_d C_d} \]

\( t_d \) is the time to detect a security incident. \( e \) is the same as in the previous equation. \( \alpha_d C_d \) is the cost of investing in a detective security measure.
Equation 12 (Financial loss including equations 10 & 11)

\[ L = L_1 \cdot \alpha \cdot e^{-\alpha C_c} + L_2 \cdot \beta \cdot e^{-\beta C_d} + L_3 - I \]

This is the loss in equation 7 with equation 10 and 11 taken into consideration. I is when the treatment option is to transfer risk and the insurance company pays the compensation (I) to cover the loss.

Equation 13 (Security risk including equations 9 and 12)

\[ R = T \cdot \nu \cdot e^{-\nu C_p} \cdot \left[ L_1 \cdot \alpha \cdot e^{-\alpha C_c} + L_2 \cdot \beta \cdot e^{-\beta C_d} + L_3 - I \right] \]

Taking equation 9 (probability p) and equation 12 (loss L) the quantitative equation for the security risk (R) from equation 8.

Equations 14-22 is about assessing the investment return and then selection of an optimum measure.

Equation 14 (Benefit and cost)

\[ B > C \]

The point of a cost benefit analysis is to compair the cost of certain activities with the benefits that the activity provides. B is benefits and C is costs. The variable B should be greater than C for the introduction of the security activity to be reasonable.

Equation 15 (Benefit)

\[ B = R_0 - R(C) \]

The benefits are generally viewed as cost-savings by reducing the probability of an incident or reducing the consequences. B equal to the risk reduction due to the implementation of a
security measure. In this equation B is calculated as the difference between the risk levels before the introduction of security measure R(C).

**Equation 16 (ROI)**

\[
ROI = \frac{B - C}{C}
\]

This equation calculates the return of the investment. It compares the benefits with the costs and the result is the investment profitability expressed in percentages, a positive value meaning that the investment is justified.

**Equation 17 (Example of ROI)**

\[
ROI = \frac{\text{€8,750} - \text{€3,400} - \text{€1,600} - \text{€450}}{\text{€1,600} + \text{€450}} = 160\%
\]

Equation 17 is an example of equation 16.

**Equation 18 (ROI for preventative security measure)**

\[
ROI = \frac{T \cdot v (1 - v^a C_p) \cdot L - C_p}{C_p}
\]

This is how the ROI is calculated with a preventive security measure which reduces the vulnerability.

**Equation 19 (ROI for corrective security measure)**

\[
ROI = \frac{T v L t^{-\alpha} (1 - e^{-\alpha C_c}) - C_c}{C_c}
\]

This is how the ROI is calculated with a corrective security measure which reduces the financial loss.
Equation 20 (ROI for transfer of risk)

\[
ROI = \frac{TVI - C}{C}
\]

Transfer of risk to for example an insurance company is considered a corrective security measure since it doesn’t reduce the incident probability, it only mitigates the consequences. This is another expression of equation 16 with transfer of risk.

Equation 21 (NPV)

\[
NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + i)^t}
\]

In case of long-term investments, NPV is considered to be better. NPV discounts all the anticipated benefits and costs to current value and the benefits and costs are expressed in a monetary unit. i is the discount rate. The investment is justified when the result is equal to or greater than zero.

Equation 22 (IRR)

\[
\sum_{t=0}^{n} \frac{B_t - C_t}{(1 + IRR)^t} = 0
\]

This calculates the IRR which makes it possible to find the discount rate at which the NPV equals zero. The IRR sets the discount rate at which the present value of inflows equals the present level of outflows.

Comparing security measures

The way that CBA is used in this study, the security measures are compared through ROI, NPV and IRR. Generally, the preferred security measure from an economic view is the one with the highest ROI, NPV and IRR. The measures can be in favor of different security measures. When
that happens, the decision will be made on subjective terms. Although for many, the ROI results are what the decisions are based on. According to a survey done by CSI (2011: 22), 54% of the respondents use ROI, 22% use NPV and 17% use the IRR [5].

**ROI (Return of Investment)**

ROI is popular when it comes to measuring business investments. It defines how much an organization gets for the money that they spent on a certain business investment. When you compare business investments through ROI, you can calculate on which of the investments give the organization most value. The indicator is a percentage of the returned investment on a specified period of time. The way that the ROI is calculated is by dividing the present value of accumulated net benefits over a certain time with the initial cost of the investment [17].

**NPV (Net Present Value)**

NPV is the difference between the present value of cash inflows and the present value of cash outflows over a period of time. A positive NPV means that the investment earns the company more money than it costs. ROI can be problematic with long time investments and time aspects and NPV can be used for that purpose. NPV is used to compare benefits and costs during different time periods. The anticipated benefits and costs are discounted to today’s value. The benefits and costs are in that case expressed in monetary units such as euro or dollars [5].

**IRR (Internal Return Rate)**

IRR is used to find the discount rate where NPV equals zero, which means that IRR sets the discount rate at which the present value of inflows equals the present value of outflows [5]. Mathematically, it is defined as the interest rate that equates the present worth of a series of cash flows to zero. It can define the return achieved by an investment and it is often viewed as a way to measure efficiency [23].
Research method

The research method I have chosen is Action Design Research. The definition of ADR according to Sein et al., (2011: 7):

“ADR is a research method for generating prescriptive design knowledge through building and evaluating ensemble IT artifacts in an organizational setting”. [7, page 40]

ADR deals with two different challenges: Addressing a problem situation in a specific organization by intervening, evaluating, constructing and evaluating an artifact that addresses the problems in the encountered situation [7].

I have chosen this research method since it is suitable for the purpose of this thesis. SEB Kort has encountered a problem what will be addressed in this thesis. I will do so by evaluating there problem and constructing an artifact that will address their problem. The artifact that will be the result of this thesis will be a method for conducting structured and cost-effective risk management which will solve the problem at SEB Kort.

I have chosen ADR because the purpose of this thesis is to combine to methods and propose a hybrid method that can be used for risk management with a cost-benefit perspective. I have not found such a method that I can use which is why I will not do a case study in SEB Kort with an existing method. The coat hanger model will also be used as guidance for how to create theories from practice; the model will be presented later in further detail in an upcoming section.

The steps in ADR are:

1. Problem formulation. The problem that this study aims to solve is clearly defined and based on original sources. The problem has been defined through literature review and through an interview. One interview is conducted in this step, with the CISO at SEB Kort.

2. Building, intervention and evaluation.
This work has been an iterative process in many ways. The implementation of IRAM2 was an iterative process where we had to go back and forth between the phases to be able to adjust the result in a way that suited the purpose. It wasn’t decided in the beginning where to add CBA to IRAM2, this is something that was tested during the process. I evaluated after each phase of IRAM2 if I had enough information or not to start with CBA and choose where it suited best. The CBA method was implemented and evaluated, and then implemented again with changes that solved problems that where encountered the first time. In the whole process, each phase in IRAM2 or step in CBA has been evaluated to see if there is any room for improvement or if any changes need to be done to the methods. The pros and cons have been evaluated to find ways to improve the methods. The intervention has been done by implementing and “testing” the two chosen methods at SEB Kort and evaluating how it worked and what can be changed in those methods to make them better. These steps are documented in a chronological order. In the evaluation, the CISO will be interviewed. He is the one that has given me the assignment of doing the risk management work at SEB Kort. The IT manager will also be involved to be able to objectively evaluate the result and see if it was useful for SEB Kort. The IT manager is the decision maker when it comes to IT investments which includes investments in security and is therefore a good candidate for evaluating the results. The results will be evaluated through interviews with the IT manager and CISO as well as a documentation of my experiences and conclusions from working with the methods. The coat hanger model is also used to evaluate the work in an objective way by providing a clear framework to how it should be done. In this way the coat hanger model will help with the evaluation step of ADR.

3. Reflection and learning. This is something that is done continuously during the first steps of ADR and afterwards. There have been learning and reflections during the process to be able to change the way of working. Two interviews have been done to get input for the evaluation. The interviews are with the CISO and IT manager. Those interviews will provide input about reflections and learning from their perspective.
4. Formalization of learning. The problems that have been encountered will be generalized to the extent possible by building the new method. A set of design principles that can be used when combining traditional risk management with CBA has been created.

**Other methods**

“Action research combines theory and practice through change and reflection in an immediate problematic situation within a mutually acceptable ethical framework.” [25, page 94]

Action research is an iterative process and contains problem diagnosis, action intervention and reflective learning [25]. Action research could be used for this study since the purpose of action research is combining practice and research. It is also about implementing research and theories in to practice which is suitable for this study. Researchers that work with action research help solve an organizational problem which is what this study aims to do. The reason that action design wasn’t chosen is because the way that I will try to solve an organizational problem is through design, which is not the expected result of action research. ADR includes designing an artifact to solve a problem in an organization, which is what this study is seeking to do and that is the reason ADR is chosen.

With quantitative research, the aim is to determine the relationship between things in a population. Quantitative approaches can be either descriptive or experimental. For an accurate estimate of a relationship between different variables in descriptive research, there usually needs to be a sample of hundreds or even thousands of subjects [24]. Getting data from hundreds or thousands of people does not suit the purpose of this study, which needs a more detailed in depth analysis. Quantitative research is about quantifying relationships and often providing statistics [24]. This study is about getting a deep understanding of risk management methods and the result is expected to be evaluations and design, rather than statistics which is the case for quantitative studies. A quantitative approach would not be suited for evaluating methods since I will need to go in depth to be able to analyze the methods and find ways to combine and improve them.
Coat hanger model

The coat hanger model that is developed by Päivärinta and Smolander [27] will be used as a guideline for evaluating the implementation done to get an objective and scientific evaluation. The coat hanger model is a process of building theories from practices. It was developed for software engineering but can be used generally for creating theories. The model builds on six main concepts that are used to build theories: learning, a practice, development context, rationale, impact and theory. The coat hanger model can be used as an analytical tool for discussing a hypothesis and developing a theory. The model will in this case be used as a guideline to develop a theory (the hybrid method) and to have an analytical way to evaluate it. Depending on the purpose and how the work is being conducted, the process can start in different stages of the coat hanger model.

Practice/practicing

In the dictionary, the definition of practice is “something people do regularly” [29]. In an organizational context, it can be defined as the organizations routine use of knowledge, especially “know-how” [31]. There is a concept of “best practice” which means the best routine
for use of knowledge, and that means that lessons learned from practice can be transferred between organizational contexts and over time. According to Päivärinta and Smolander (2013:27) practice descriptions and definitions can be useful when it comes to analyzing current actions in context and being able to learn from them.

**Espoused practice/adopting**

The espoused practice is what is being developed or created. The practice is the starting point and what is expected to be adopted. For many reasons, the implementation is not always performed as planned and the actual implementation and what is actually done is the espoused practice.

**Rationale/rationalizing**

Rationale is both useful for modification and argumentation of the methods used in an organization and for understanding an organization’s practices in general. Rationale can be used to justify the use of a practice.

**Lessons learned/learning**

The coat hanger model is based on the general idea of learning. The definition of learning used is in an ISD context is that to be able to learn from practice, we have to identify or assume causal relationships between actions during ISD and the desired outcomes [28]. Learning can be defined as “The acquisition of knowledge or skills through study, experience, or being taught.” [30, page]

**Impact/ evaluating**

Every organization needs to evaluate to be able to learn from their experiences. The impacts of the practices need to be analyzed. The impacts of the previous practices can be used as input for adjusting the practices [27].
Theories/theorizing

All of the concepts mentioned earlier are needed for creating and evaluating theories. According to Päiväranta and Smolander (2013:27) it is useful to analyze the practice and try to produce predictive theories, with regard to their impact on processes and contexts.

Why CBA and IRAM2?

The reason that I choose IRAM2 as a risk management method was mainly because SEB has chosen it as a method for their risk management work. One of my purposes is to help SEB Kort with their risk management work and since they wanted me to use IRAM2, I chose to do so. IRAM2 is a complete end-to-end risk management methodology that covers all steps in the risk management process and is widely used in the industry. During an interview with the CISO at SEB Kort, the CISO described that they use IRAM2 because it is a widely used standard and because they are members of ISF which have developed the method. However, IRAM2 is a method that is similar to other risk assessment methods and contains the steps that should be included in risk assessment according to Alberts and Dorofee (2002: 18). IRAM2 is used as an example of a traditional risk assessment method and can be replaced with a similar method since the general concepts and steps will be the same.

IRAM2 lacks an extensive economic aspect to not only get the best result from a security point of view but also make sure that the result is cost-effective for the organization. The reason that I choose the CBA method by Bojanc et al (2013:5) is because it is one of the few CBA methods that are dedicated for information security risk management and because it is a comprehensive method that provides a detailed analysis and covers many economic aspects of risk management work. Recently, CBA is becoming a popular method that is applied to assessment of computer-related risks. It is well established in other fields such as microeconomics and management accounting theory.

The usefulness in CBA comes from the fact that it can be used to determine estimated levels of expenditure that is appropriate for protecting assets based on their value [21]. Adding CBA to a more traditional method such as IRAM2 will add the economic incentives needed for management to further invest in security measures. On top of the comprehensive assessment
and information that IRAM2 provides, the economic benefits of investing in security measures will become clear.

**Delimitations**

The risk management only includes risks at SEB Kort and not the rest of SEB, due to limits in time and resources. The bank has over 15,000 employees (around half of them in Sweden) and many different departments that work very differently. Therefore, I have chosen to only work with one department, which is SEB Kort. The main focus has been on risks that are in some way related to information security. Since SEB Kort is a financial institution, there are several other risks such as financial risks that are relevant, which have not been considered in this research. Only information security risks have been in scope, which can also be affected by the fact that SEB Kort is a financial institution.

There has not been a focus on risks that are associated with software management and development. I have not gone into detail in each system because has not been doable within the time frames set for this research. For that reason, the risks that occur when developing a system has not been analyzed either. The evaluation is based on the systems that exist within SEB Kort today, in that they currently are in. The risk management was done on a specific project chosen by the CISO. The systems that have been in scope are the ones that are affected by the project being evaluated.

Some significant risks to address have been chosen together with the CISO at SEB Kort. Those risks where found trough implementing IRAM2. One of the purposes of this paper is to help SEB Kort with their risk management work and therefore, the CISO has had a big role in choosing which risks to focus on based on the organization’s needs and his knowledge about the. The costs and benefits of those risks have been through CBA. There are a lot of risks for an organization like SEB Kort due to the sensitive data that they have and because it is such an IT heavy organization. Because of that and time limitations, some significant risks to analyze will be chosen and some of the risks will be out of scope. The focus has been on risks with high vulnerabilities that IRAM2 shows need to be mitigated.
**Expected results**

The expected results are both practical improvements for SEB Kort and also a contribution to the research field. The expected practical results at SEB Kort is that they will get help with starting to adopt a risk management method and that they can start their part in the journey that SEB as a whole is going through with finding a common way of working with information security risk management. The unified way of working is expected to lead to better communication between departments and with management about security investments. Always using the same standards and methods in risk management will also lead to more even quality in the results and it will not be as dependent on the person conducting the risk management. The method will be tailored to fit real organizational needs and simplified where it needs so that organizations will have a better chance at being able to adopt it in practice.

In the theoretical field, the study is expected to provide a hybrid method that has the benefits of IRAM2 and CBA and that can be useful in the information security field in general and not limited to financial institutions. Using CBA together with a more traditional comprehensive information security risk management method will fill a knowledge gap in the field.

**Risks**

- The equations in the CBA analysis being too complex
- The values needed in the CBA analysis will be difficult to estimate
- Difficulties in getting the time needed from the involved employees at SEB Kort, mainly the CISO
- Difficulties in scoping which risks to involve and choosing risks to calculate in CBA analysis
- Difficult to get a good overview of the risks at SEB Kort due to lack of work in the area before and many different risks depending on where in the organization you look
• There will not be enough time to go through the CBA analysis for several risks

• Problems with combining two methods that are not meant to be used together

Some of these risks are difficult to prevent. To avoid problems with the CBA analysis I am trying to prepare as much as I can by going through the steps in the analysis and making sure they are doable. There is always a risk with estimating values and the difficulty to set them to a precise value. That will with all certainty occur in this case and it is an issue that is difficult to solve in the frames of this thesis. It can be handled by accepting that the values we estimate won’t always be completely and can’t be expected to be.

The CISO at SEB Kort will be helpful in getting an overview of the risks and choosing which risks are significant and should be in scope. It also depends on which risks they are interested in having in scoping because of their business interests. There can be problems with combining the methods since they have different suggestions on how to execute some of the steps in risk management. I might be able to combine the methods and get a more valuable than I would if I only used one of them. My conclusion might also be that the two methods are not suited to be used together.
Result

The following is a presentation with results of the implementation of IRAM2 and CBA. There are also descriptions of how each step was implemented. The evaluation of the implementation that was conducted through interviews with the organization is also presented. There is a suggestion for a hybrid method and a description of how that method works.

IRAM2

Phase A: Scoping

Single Trans With Vendor – phase 1 & 2

This figure is a technical view of the flow that is being assessed. The parts within the green lines are the parts that will be in scope. The rest of the information flow is left unchanged and will therefore not be assessed.
Figure 7, New flow introduced

Figure 7 illustrates the new information flow with virtual cards being introduced and that is being assessed. CSP is the vendor service settlement platform.
## Profiling

### The organizational

<table>
<thead>
<tr>
<th>Organizational</th>
<th>Comments</th>
<th>Potential Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial intellectual property (CI)</td>
<td>The commercial IP of the target organization is highly valuable to potential buyers.</td>
<td>How valuable is the organization's commercial IP to potential buyers?</td>
</tr>
<tr>
<td>Public sector intellectual property (PSI)</td>
<td>The organization does not explicitly define public sector intellectual property (PSI).</td>
<td>How valuable is the organization's PSI to potential buyers?</td>
</tr>
<tr>
<td>Goods or services</td>
<td>Highly valuable</td>
<td>How valuable is the organization's goods or services to potential buyers?</td>
</tr>
<tr>
<td>Public interest</td>
<td>Operates critical public infrastructure</td>
<td>To what extent does the organization control or operate critical public infrastructure?</td>
</tr>
<tr>
<td>Sectoral political influence</td>
<td>Moderate influence</td>
<td>To what extent does the organization yield sectoral political influence?</td>
</tr>
<tr>
<td>Brand reputation</td>
<td>Strong reputation</td>
<td>How strong is the organization's brand reputation?</td>
</tr>
<tr>
<td>Organizational performance</td>
<td>Strong performance</td>
<td>How strong is the organization's performance?</td>
</tr>
</tbody>
</table>

### The environmental perspective

<table>
<thead>
<tr>
<th>Environmental factors</th>
<th>Potential Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economy</td>
<td>What are the prevalent economic factors?</td>
</tr>
<tr>
<td>Political</td>
<td>Government policies, voting, lobbying, political climate, internal political issues, international relationships, corruption</td>
</tr>
<tr>
<td>Legal &amp; Regulatory</td>
<td>Financial insolvency, data protection, Swedish law, EU directives and regulations, Payment Card Industry Data Security Council (PCI DSS)</td>
</tr>
<tr>
<td>Climate</td>
<td>Are any organizational locations exposed to natural disasters?</td>
</tr>
</tbody>
</table>

### Business Service

<table>
<thead>
<tr>
<th>Business Service</th>
<th>Comments</th>
<th>Potential Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of business services</td>
<td>The business service provides payment solutions for both corporate and private customers (Carding) and internal accounts.</td>
<td>What function does the business service perform, and what value does it provide?</td>
</tr>
<tr>
<td>Business processes: core service</td>
<td>Card payments in store and online, authentication, card lifecycle management, fraud prevention, risk management</td>
<td>What are the business processes that are used to deliver the business service(s)?</td>
</tr>
<tr>
<td>Customer-facing/middle/back office</td>
<td>Office private and corporate networks and cloud-based front-end systems</td>
<td>Who are the customer(s) of the business service(s)?</td>
</tr>
<tr>
<td>Key supporting technologies</td>
<td>Authentication and clearing, card lifecycle management systems, fraud prevention systems, subscription systems, pay-per-use, API, travel accounts, data warehouse, customer systems, credit risk system, transaction systems, database, PATS, services, SWIFT</td>
<td>What technology is used to deliver the business service(s)?</td>
</tr>
<tr>
<td>Technology Service</td>
<td>Comments</td>
<td>Potential Considerations</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Description of technology service/system</td>
<td>Card payments for private and corporate customers in-store and online, the value the ability of the customers to pay payments anywhere in the world.</td>
<td>What function does the technology service serve, and what value does it provide?</td>
</tr>
<tr>
<td>Business processes supported</td>
<td>Authorization, Clearing &amp; Settlement, Support for customer, Fraud prevention, Card application management</td>
<td>What are the business processes that are supported by the technology service?</td>
</tr>
<tr>
<td>Importance of solution to business processes</td>
<td>The technology service is critical to the business service.</td>
<td>How important is the technology service to the business process(es)?</td>
</tr>
<tr>
<td>Financial transactions</td>
<td>Significant level of financial transactions.</td>
<td>What level of financial transactions is the technology service involved in?</td>
</tr>
</tbody>
</table>

### Architectural Considerations

<table>
<thead>
<tr>
<th>Architectural Considerations</th>
<th>Comments</th>
<th>Potential Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural description</td>
<td>Three-tier architecture, Java, Cobol, .Net, Assembly, EF, remotes, Windows, Linux, Unix, DB2, Oracle, SQL, Cryptography functions</td>
<td>What is the architecture of the technology service (e.g., two-tier, three-tier), technology platform being used, etc.</td>
</tr>
<tr>
<td>Organizational familiarity with technology</td>
<td>No, it is new</td>
<td>Is the technology used for this service new to the organization, or has it already been deployed successfully for other technology services?</td>
</tr>
<tr>
<td>Number of interfaces</td>
<td>More than 10</td>
<td>How many interfaces does the technology service/application have?</td>
</tr>
<tr>
<td>Interfaces with business critical systems</td>
<td>Yes</td>
<td>Does the application or technology service have an external interface with other business critical technology services or applications?</td>
</tr>
<tr>
<td>Support arrangements</td>
<td>Combination in-house and vendor</td>
<td>How is the technology supported?</td>
</tr>
</tbody>
</table>

### User Profiling Considerations

<table>
<thead>
<tr>
<th>User Profiling</th>
<th>Comments</th>
<th>Potential Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of users</td>
<td>Approximately 3.5 million users</td>
<td>How many users are there of this technology service?</td>
</tr>
<tr>
<td>Groups/types of users</td>
<td>Private customers, Corporate customers, Business administrators, System administrators, Developers</td>
<td>What are the typical types or groups of users that are going to be interacting with the system?</td>
</tr>
<tr>
<td>Location of users</td>
<td>Anywhere in the world, combination of internal and external</td>
<td>Where are the users of the technology service located?</td>
</tr>
</tbody>
</table>

---

**Figure 8, Profiling environment part 1**

**Figure 9, Profiling environment part 2**
Step 1, developing a profile for the environment is shown in figure 8 and 9. This phase was conducted together with the CISO at SEB Kort and the IT architect from the project. The CISO was helpful with profiling the environment since he has a holistic view of the organization and the security situation. The step was about seeing the organization and the country and environment that the organization exists in from a risk point of view. The questions were at a very high level meaning that it does not dive into any details. In our case, this step did not provide any relevant information for the risk assessment of this particular process. In my opinion, this is relevant when you want to do a risk assessment of an organization in general. This is a relevant evaluation to do for all organization but does not need to be a part of the risk assessment of each specific process. If it is used in a more level risk assessment like mine, it can be re-used for the coming assessments since it is at such a high level and describes the organization in general. The phase was done without any problems or difficulties but didn’t provide much valuable information either.
Step 2, scoping the assessment is shown in figure 12 and 13. This step was done together with the IT architect of the project and the CISO. This step was necessary to define boundaries on what to assess and not start a risk assessment that would become too big to handle. When scoping we left out the systems that wouldn’t be changed or affected by this new information flow. The authorization and integration systems are complex and fragile systems and need to be risk assessed individually. Their part of the information flow will be the same as before and we choose to only take the systems that will be changed in any way into scope. In this phase, we also identified key stakeholders, which were valuable for the next steps where their input was needed. Their names have been removed for integrity purposes.
## Phase B: Business Impact Analysis

### IRAM₂ Business Impact Assessment (BIA)

#### Confidentiality

<table>
<thead>
<tr>
<th>Information Asset</th>
<th>Impact</th>
<th>Realistic</th>
<th>Impact Test</th>
<th>Worst-case</th>
<th>Impact Test</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems documentation</td>
<td>Financial</td>
<td>Negligible</td>
<td>Negligible in losses, order or contract loss</td>
<td>Low</td>
<td>Negligible in losses, order or contract loss</td>
<td>Most information on the system documentation may make it easier to perform fraud or sabotage. The security should not depend on the design of solutions or protocols. There might be intellectual property.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Operational</td>
<td>Negligible</td>
<td>Negligible in the loss of management's ability to effectively govern or operate the organization</td>
<td>Low</td>
<td>Negligible in the loss of management's ability to effectively govern or operate the organization</td>
<td>Limited system documentation will not affect any operational functions. System documentation cannot be replaced in this case.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Legal and Regulatory Compliance</td>
<td>Negligible</td>
<td>Negligible in the loss of organizational operations, or relationship with regulator(s)</td>
<td>Negligible</td>
<td>Negligible in the loss of organizational operations, or relationship with regulator(s)</td>
<td>There are no regulatory or legal impacts when losing system documentation.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Reputational</td>
<td>Negligible</td>
<td>Negligible in the loss of public reputation</td>
<td>Low</td>
<td>Negligible in the loss of public reputation</td>
<td>Customers will probably not be interested in the loss of a single system documentation. If this is the case, the number of customers that must be expected to follow.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Health and Safety</td>
<td>Negligible</td>
<td>Negligible in the injury or death to one individual</td>
<td>Negligible</td>
<td>Negligible in the injury or death to one individual</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Figure 11, BIA Confidentiality**
## IRAM: Business impact assessment (BIA)

### Integrity

<table>
<thead>
<tr>
<th>Information Asset</th>
<th>Impact</th>
<th>Realistic</th>
<th>Impact Test</th>
<th>Worst-case</th>
<th>Impact Test</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>System documentation</td>
<td>Financial</td>
<td>Negligible</td>
<td>Low</td>
<td>High (significant financial loss)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System documentation</td>
<td>Operational</td>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>High (loss of competitive advantage)</td>
<td></td>
</tr>
<tr>
<td>System documentation</td>
<td>Legal and Regulatory Compliance</td>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>No regulatory or legal impacts</td>
<td></td>
</tr>
<tr>
<td>System documentation</td>
<td>Revenue</td>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>Will probably not impact our firm in any significant manner</td>
<td></td>
</tr>
<tr>
<td>System documentation</td>
<td>Health and Safety</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 12, BIA Integrity**
In this phase, I got help from an SEB Kort IT architect, the CISO and most of all the business SME. The information assets involved in the flow were identified. Every information asset was assessed through different perspectives. We looked at the confidentiality, integrity and availability of the data to determine the business impact through those perspectives. We have identified consequences with data not being confidential, correct or available. The consequences are operational, reputational, legal and financial. Health and safety consequences are also included in the original BIA as IRAM2 intended but was not relevant for this BIA since there were no such consequences identified. This phase lays the groundwork for the rest of the risk assessment. We identify what we are trying to protect and why. We also identify what can happen if we don’t protect it properly, both in a realistic scenario and in a worst case scenario. This phase took a bit of time to do and both people with technology and business skill need to be involved. However, the phase is necessary to continue with the risk assessment.

<table>
<thead>
<tr>
<th>Information Asset</th>
<th>Impact</th>
<th>Realistic</th>
<th>Impact Test</th>
<th>Worst-case</th>
<th>Impact Test</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems documentation</td>
<td>Financial</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Financial consequences may be financial, operational, reputational, legal, and financial.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Operational</td>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Systems documentation is not available or system documentation is not available.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Legal and Regulatory Compliance</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td>No regulatory or legal impacts.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Reputational</td>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>IRAM2 intended but was not relevant for this BIA since there were no such consequences identified.</td>
</tr>
<tr>
<td>Systems documentation</td>
<td>Health and Safety</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Negligible</td>
<td>No consequences identified.</td>
</tr>
</tbody>
</table>

**Figure 13, BIA Availability**
and be aware of the assets the risk assessment wishes to protect. The health and safety impacts were determined not to be relevant for this project and therefore they are all not applicable. In the figures above, I have shown the BIA with system documentation as an example. The BIA is done for all information assets. Because system documentation was one of our less vulnerable information assets, I have used it to show how the BIA was done.

**Phase C: Threat Profiling**

<table>
<thead>
<tr>
<th>Adversarial</th>
<th>Include adversarial threats:</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Origin</td>
<td></td>
</tr>
<tr>
<td>Competitor</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Employee (general)</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td>Employee (privileged)</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td>Hacking group</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Individual hacker</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Nation-state</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Organised criminal group</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Supplier/vendor/partner</td>
<td>External</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accidental</th>
<th>Include accidental threats:</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Origin</td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td>External</td>
<td></td>
</tr>
<tr>
<td>Employee (general)</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td>Employee (privileged)</td>
<td>Internal</td>
<td></td>
</tr>
<tr>
<td>Supplier/vendor/partner</td>
<td>External</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 14, Threat profiles that were included**
This phase was done in collaboration with the CISO, and we had some help from one of the developers that has been involved in the project. In the figures above, I have shown the threat profiles that we used. All of the threat profiles shown are from IRAM2 material. We chose to use the threat profiles as is for accidental and adversarial threats and didn’t add or remove anything. We did however not include the environmental threats because we chose to leave environmental threats and threat events out of scope in the previous phases. This is because we feel that environmental risks should be considered for the whole organization on a higher level and not for a specific project. We also do not operate in a country where natural disasters occur. Not to say that it is impossible but we didn’t feel that it was relevant for this risk assessment. In my opinion, doing a risk assessment for environmental risks should be done separately and on a higher level, for the entire organization.
The CISO and I profiled the threats and their attributes based on our knowledge of these threats and their interest in us. The threat profiles are analyzed based on history, culture, privilege and competence. This phase can also be considered general and can be re-used in other projects in the same organization. It is a good way to get an overview of the adversarial threats but it also highlights the accidental threats that might get forgotten otherwise.

In this phase we also chose which threat events are relevant to our project that we are evaluating. ISF then creates a prioritization list of threat profiles based on the attributes we have listed and creates values for their likelihood of initiation and threat strength. Then, the threat profiles are mapped with the chosen threat events. We also mapped the information assets that can be impacted by each threat event. This is very helpful because it lets us prioritize and focus on the right things in a systematic and objective way. The result of this step was that we got an understanding of the threats and their related threat events and also how they could affect our different information assets. The threat events that required higher threat strength than the threats actually had are excluded because those threats wouldn’t occur according to this method.

Phase D: Vulnerability assessment

<table>
<thead>
<tr>
<th>Control reference</th>
<th>Control title</th>
<th>Description</th>
<th>Control type</th>
<th>Mitigates likelihood or impact</th>
<th>Control effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN001</td>
<td>Secure network design</td>
<td>Organizational networks should be securely designed, including: • separating sensitive/critical internal business systems and traffic from less-sensitive/external network; using firewalls or equivalent; • securing the perimeter of the network using firewalls or equivalent in such a fashion as to limit the exposure of applications and infrastructure to only those services that are required to be provided externally • using secure versions of critical services (e.g. MD5 instead of DNO and IPS)</td>
<td>Preventative</td>
<td>Likelihood and impact</td>
<td>Effective</td>
</tr>
</tbody>
</table>

Figure 16, Example of control effectiveness
In this phase, I got help from the same people as in the last phase, the CISO and the developer. We have assessed our effectiveness with different controls to determine how vulnerable we are to different threat events. The controls are from a list in the IRAM2 materials. ISF has a list of controls that are linked to each threat event to show which threat events the control mitigates.

The result from this step is essential to figuring out where we need to improve our controls and security mechanisms, which is one of the most important outputs of the risk assessment. Each control that is relevant for the prioritized threat events are evaluated. In the picture above, an example is shown on a control and its chosen control effectiveness. The control strength is then set for each risk and where the control strength is low and it is linked to an in scope threat event, a vulnerability is found. An example of this is found in the second picture above.

**Phase E: Risk Evaluation**

This phase has been done without involvement from the organization. With the information I gathered in the previous step and the knowledge I have of the organization, I felt comfortable doing it alone. This step summarizes the information from the previous steps and formulates the final risks. In the picture above I have shown what information there is about each risk. Because the information in this step contains details about the risks, I have chosen not to show an example containing information. Most of the data is derived from previous steps and some are set manually based on the summarized information about the risk and the control strength. The residual risk rating is the output of this step and is also the base for the next step.
Phase F: Risk Treatment

This step was done in collaboration with the CISO. We determined for each risk if it exceeds the risk appetite or not. Then we decided which treatment option to choose. The options for treatment are mitigate, accept, avoid or transfer. There was also a possibility to write the status and who the owner of the actions is. We also wrote a target date for when the actions should be done according to us. This is the final step in IRAM2 and is what concludes all the work done previously. It was good that we had to determine the person responsible when the deadline is. This prevented the risk assessment only being something that lies in a desktop drawer and never leads to any activities. However we will have to follow up on the activities to make sure that the activities are done by the deadline. Phase E and F are done iteratively. In phase E the risks that need to be mitigated are identified and in phase F the decision should be made regarding which risk treatment to choose. Here, there is a need to go back and forth between phase E and F to see which control measures are related to that risk, which controls do we need to improve and which ones are economically effective.

CBA

The values are set based on conversations with representatives of the organization. Some of the values are fictive due to confidentiality. The threat that I have chosen to evaluate with CBA is “Insert malware into information systems” because it was the highest prioritized risk in the result from IRAM2.

Calculating the risk

Case Study

This case study is mostly based on the equations. Some of the values are set in this step such as max/min risk. The result is to be considered fictitious due to the confidentiality in the true
numbers. This case study is only here to present the principles of how to calculate and evaluate the benefits and returns on investments made.

Maximum risk $R_{\text{max}} = €100,000/$year
Maximum loss $L_{\text{max}} = €500,000$
Minimum risk $R_{\text{min}} = €10/$year

- $v = 0.1$
- $T = 0.6$
- $\rho = 0.06$
- $t_{\text{r0}} = 16$ hours
- $t_{\text{d0}} = 2$ hours
- $L_1 = €80 /$hour
- $L_2 = €27 /$hour
- $L_3 = €360,000$
- $L = €361,345.72$

**Measure A – Antivirus**
Cost assessment

Initial cost: €10,000
Annual upgrade: €200
Annual maintenance: €100
Productivity: 0.8

Economic evaluation

<table>
<thead>
<tr>
<th>Year</th>
<th>Discount rate</th>
<th>Benefits</th>
<th>Purchase and upgrade costs</th>
<th>Maintenance costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>10,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0.05</td>
<td>20813.52</td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>0.05</td>
<td>20813.52</td>
<td>200</td>
<td>100</td>
</tr>
</tbody>
</table>
Measure B – Security testing

Cost assessment
Initial cost: €0
Annual upgrade: €3000
Annual maintenance:
Productivity: 0.9

Economic evaluation

<table>
<thead>
<tr>
<th>Year</th>
<th>Discount rate</th>
<th>Benefits</th>
<th>Purchase and upgrade costs</th>
<th>Maintenance costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.05</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0.05</td>
<td>23415.21</td>
<td>3000</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0.05</td>
<td>23415.21</td>
<td>3000</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0.05</td>
<td>23415.21</td>
<td>3000</td>
<td>0</td>
</tr>
</tbody>
</table>

Equation 1

The first equation is about calculating P (probability of a security incident occurring). T is the threat probability, in IRAM2 called likelihood of initiation. IRAM2 has shown that for this threat, the Loi is high. Taking that into consideration together with information about how often malicious individuals try to infect us with malware, the value of T is set to 0.6 (T should be between 0 and 1). v is the vulnerability and is set by taking the control strength of IRAM2 into account together with information about past attacks and success rates. V is also a value between 0 and 1 where 0 is completely secure. V is set to 0.1.

\[ \rho = T \cdot v \]

T = 0.6
v = 0,1
ρ = 0,6 * 0,1
ρ = 0,06

Equation 2

\[ L = L_s + L_r(t) + L_i(t) + L_p(t) + L_{SLA} + L_{indirect} \]

L is the financial loss due to a security incident. To calculate it, the other values must be set first. They will be calculated in the next equations (3-7).

\[ L_s = €10.000 \]

Equation 3

\[ L_r(t) = n \cdot p \cdot t_r \]

n = 12
p = € 80/h
\( t_r = 16 \) h

\[ L_r(t) = 12 \cdot 80 \cdot 16 \]

\[ L_r(t) = €15360 \]

The cost of repairs will be €15630 in total.

Equation 4

\[ L_i(t) = EF_i \cdot i \cdot (t_r + t_d) \]

EF_i = 0,001
\[ i = 1500/\text{h} \]
\[ t_r = 16\text{h} \]
\[ t_d = 2\text{h} \]
\[ \text{Li}(t) = 27 \]

This means that the corporate income loss is €27/h.

**Equation 5**

\[
L_p(t) = m \cdot \text{EF}_p \cdot p' \cdot (t_r + t_d)
\]

\[ m = 12 \]
\[ \text{EF}_p = 0.6 \]
\[ p' = 80/\text{h} \]
\[ t_r = 16\text{h} \]
\[ t_d = 2\text{h} \]
\[ \text{Lp}(t) = 10368 \]

The productivity loss is €10368/h.

**Equation 6**

\[
L = L_s + n \cdot p \cdot t_r + \text{EF}_i \cdot i \cdot (t_r + t_d) + m \cdot \text{EF}_p \cdot p' \cdot (t_r + t_d) + L_{\text{SLA}} + L_{\text{indirect}} = (n \cdot p + \text{EF}_i \cdot i + m \cdot \text{EF}_p \cdot p') \cdot t_r + (\text{EF}_i \cdot i + m \cdot \text{EF}_p \cdot p') \cdot t_d + L_s + L_{\text{SLA}} + L_{\text{indirect}}
\]

\[ L_{\text{SLA}} = \text{€100,000} \]
\[ L_{\text{indirect}} = \text{€250,000} \]
(12 \times 80 + 0.001 \times (1500 + 12) \times 0.06 \times 80) \times 16 + (0.001 \times (1500 + 12) \times 0.6 \times 80) \times 2 + 10000 + 100000 + 250000 = 22757 + 1182 + 360000 = 361345.72

\[ L = \varepsilon 361.345,72 \]

**Equation 7**

\[ L = L_1 + t_r + L_2 + t_d + L_3 \]

This is a simplified version of equation 6, L is still \( \varepsilon 361.345,72 \).

**Equation 8**

\[ R = \rho \cdot L = T \cdot v \cdot \left[ L_1 \cdot t_r + L_2 \cdot t_d + L_3 \right] \]

\[ R = \rho \times L = 0.06 \times 361345.72 = \varepsilon 26.016,9 \]

The total risk for the project being evaluated is \( \varepsilon 26.016,9 \).

**Selecting the optimum measure**

The security measures we have chosen is anti-virus and security testing which are labeled as preventative security measures. Therefore, some of the equations for other types of security measures will be skipped. The calculations in the coming section are the ones for preventive security measures. The equations for preventive, detective and transferring risk will not be calculated. Further on, the calculations will be done twice, once for each security measure.

**Measure A - Antivirus:**

**Equation 18**

\[ ROI = \frac{T \cdot v \left(1 - v^{a_p} c_p \right) \cdot L - C_p}{C_p} \]
This equation will be modified since it was discovered that the specified conditions for
equation 9. Which this equation is built upon, was not satisfied even though it was claimed.

The following condition:

\[ \lim_{c \to \infty} \rho(T_c \nu C_p) = 0. \]

Is not true. Since \( \alpha \) and \( C > 0 \) this condition will not converge towards 0 if \( C_p \to \infty \).

Therefore the benefit:

\[ T \cdot \nu (1 - \nu^{a_p c_p}) \cdot L \]

Will be calculated using this equation instead:

\[ B = ALE_0 \cdot ALE_S \]

\[ ALE_0 = L \cdot ARO \]

\[ ALE_S = (1 - r) ALE_0 \]

\[ ARO = \rho \]

\[ r = \text{Risk reduction, } 1 > r > 0 \]

\( r \) for Antivirus will be set to 0.8 meaning that the risk will be reduced by 80% by implementing
Antivirus.

\[ B = 26016.9 - ((1-0.8) 361.345,72) \]

\[ B = 20813.52 \]

\[ ROI = \frac{B - C_p}{C_p} \]

\[ ROI = 20813,52-10000/10000 \]

\[ ROI = 1,08 = 108\% \]
Equation 21

\[ NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + i)^t} \]

\( i = 0.05 \)

\( n = 4 \)

\( B = 20813.52 \)

\( C = 10000 \)

\( C_a = 300 \)

\[
NPV = \left( \frac{20813.52 - 10000}{1+0.05} \right) + \left( \frac{20813.52 - 300}{1+0.05} \right) + \left( \frac{20813.52 - 300}{1+0.05} \right)^2 + \left( \frac{20813.52 - 300}{1+0.05} \right)^3 = 10298 + 18606 + 17720 + 16876
\]

\( NPV = 63500 \)

Equation 22

\[
\sum_{t=0}^{n} \frac{B_t - C_t}{(1 + IRR)^t} = 0
\]

\( IRR = 1.829 \)

Measure B - Security Testing:

Equation 18

\[
ROI = \frac{T \cdot v \left( 1 - v^a \frac{C_T}{C_p} \right) \cdot L - C_p}{C_p}
\]

The benefit:
Will be calculated using this equation instead:

\[ B = ALE_0 - ALE_S \]

\[ ALE_0 = L \cdot ARO \]

\[ ALE_S = (1 - r) ALE_0 \]

\[ ARO = \rho \]

\[ r = \text{Risk reduction, } 1 > r > 0 \]

\( r \) for Security Testing will be set to 0.9 meaning that the risk will be reduced by 90\% by implementing Antivirus.

\[ B = 26016.9 - ((1-0.9) \times 26016.9) \]

\[ B = 23415.21 \]

\[ ROI = \frac{B - C_P}{C_P} \]

\[ ROI = 23415.21 - 3000/3000 \]

\[ ROI = 6.8 = 680\% \]

\[ NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} \]

\[ i = 0.05 \]

\[ n = 4 \]

\[ B = 23415.21 \]

\[ C = 3000 \]
\[ \text{NPV} = \frac{(23415.21 - 3000)(1+0.05)^1 + (23415.21 - 3000)(1+0.05)^2 + (23415.21 - 3000)(1+0.05)^3}{(1+0.05)^4} = 72391 \]

\[ \text{NPV} = 72391 \]

**Equation 22**

\[ \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + IRR)^t} = 0 \]

\[ \text{IRR} = 1.925 \]

**CBA result**

<table>
<thead>
<tr>
<th>Measure</th>
<th>ROI</th>
<th>NPV</th>
<th>IRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (antivirus)</td>
<td>108%</td>
<td>€63500</td>
<td>182.9%</td>
</tr>
<tr>
<td>B (security testing)</td>
<td>680%</td>
<td>€72391</td>
<td>192.5%</td>
</tr>
</tbody>
</table>

In the result of the equations we can see that both of the security investments showed positive ROI, NPV and IRR values. The results show the profitability of each security measure. The ROI for both security measures say that it is an economically justified investment. NPV which compares benefits and costs and also has the time aspect also says that the investments are economically justified. The security measure with the best results is measure B so if one should be choosen between the two, it should be security testing. Security measure B got the best result in all three measurements which shows that even though both are economically justified, investing in security measure B is better, at least from an economic viewpoint. It is also clear that both security measures can be viewed as economically justified investments. If the result of one or more measurements would be negative, it would show that it might not be economically feasible to invest in that specific security measure.
Coat hanger model

The coat hanger model will here be used to evaluate and theorize the conclusions of the implementation process.

Development context

The development context has been described earlier in the literature review and in the descriptions of SEB Kort and the problems and situation there. In the theoretical area, there is not much that is pre-defined when it comes to combining traditional risk management with economic risk management. Since they are usually used separately, there is a knowledge gap. However, there are a lot of studies about different ways of conducting risk management and some about CBA. In SEB Kort, the context is that risk management in information security is not being conducted regularly in a standardized way. The focus has been on financial risks and other business risks. The organization wishes to start with information security risk management in a standardized way. Since the proposed process will not replace an existing process, not much is pre-defined. The organization is used to concepts like the importance of proper risk management and that risks should be mitigated. However, they are not used to conducting the risk management in a standardized and controlled way in the level that the information security team wishes they would.

Practice/practicing

In this case, the practices that have been found from previous research and organizations are the IRAM2 and CBA methods for risk management. Other research and methods for risk assessment have also been input to this work. Those practices were studied in the literature review process to highlight general terms and processes within risk management and also problems with the existing processes. The IRAM2 and CBA methods have been described earlier and how they are described by their authors is how they are expected to be implemented. The expected practice is to take the methods as they are but to add CBA in a certain step of the IRAM2 process. Some of the results from IRAM2 will be used as input to the CBA calculations.
Espoused practice/adopting

The espoused practice is the hybrid method that is created from IRAM2 and CBA. Two existing practices and other pre-known practices have been used as input to the new espoused practice. Both methods have to a large extent been implemented in their original form, with some changes. The biggest change from the previous practices is that the two methods have in previous cases been used separately and they have not been combined, practitioners and literature have focused one or the other. They have been used to produce input to each other and in that way get a more qualified result. Some minor changes have also been made to the methods, specifically to IRAM2. This means that the espoused practice does differ from previous practices. The plan was to combine the methods and use output from IRAM2 to CBA and vice versa. In that perspective, both methods have to a large extent been implemented as it was planned. Some minor changes were made to IRAM2 that were not initially planned for.

Rationale/rationalizing

The rationale to work with risk management is generally to get control over risks and to be able to make strategic investments and identify what to mitigate. The rationale of adopting the hybrid method is to get all of those benefits but to also make sure that the investments are cost-effective. Depending on the evaluation and what value the implementation gives for the organization, a new rationale might be that only information security aspects or economic aspects by themselves aren’t sufficient and that the combination gives more meaningful results.

Lessons learned/learning

To learn from a certain set of actions requires that the actions are treated as “experiments” that generate evidence by testing theories [28]. In this case, the experiment is implementing IRAM2 and CBA (the selected “theories-in-use”). By implementing and testing those theories and evaluating the impact of them, conclusions can be drawn. Those conclusions can be used as input for upcoming risk management implementations.

Impact/evaluating

The impact of the previous practices (IRAM2 and CBA) will be evaluated through the experiment of implementing those practices. The impacts of the previous practices will be used
as input on how to adjust those practices into the hybrid method. To evaluate the impact of the practice and the espoused practice, a few interviews with selected stakeholders will be conducted. My own experiences from the implementation will also be documented and I will do my own evaluation of how I experienced using the methods combined.

Theories/theorizing

The theory that will be created from practice is the hybrid method that is created. The hybrid method will be a new theory that is created based on earlier practices and based on adopting those practices and “experimenting”.

Suggested hybrid method

My goal has been to find a way to combine a traditional risk assessment method with a CBA to get a result that has both the information security perspective and the economic and effective perspective. This is what will provide a valuable and useable result that decision makers can make decisions based upon. Only having an information security perspective or only seeing the costs of measures without analyzing the need for it will not be sufficient for managers to be able to make the correct decisions. I choose to combine CBA with IRAM2, and also made some small changes to IRAM2. The changes I made are based on my experience from implementing the method and based on the interviews I have conducted. The purpose of all the smaller changes is to make the implementation easier and erase unnecessary steps.

The suggested method is based on IRAM2 but with changes made to the method. The changes are for two purposes; to simplify and to introduce the economic perspectives.
Phase A: Scoping

In this phase, I have removed the profiling of the environment. For most organizations, dealing with natural disasters such as tsunamis and earthquakes are a separate process and not something that should be handled in each separate risk assessment. It is mostly static information and on a higher level than this risk assessment is done. Those risks should be handled, but in a separate forum.

A1. Develop the scope for the assessment
**Phase B: Business Impact Assessment**

This phase has remained unchanged.

The steps in this phase are:

B1. Identify the information assets

B2. Assess business impact

**Phase C: Threat Profiling**

Because the environmental perspective is being left for other forums to discuss and on a higher level, the environmental threat category is also removed from this phase. Otherwise, the step is unchanged.

The steps included are:

C1. Populate the threat landscape

C2. Profile threats

C3. Produce a prioritized threat landscape

C4. Scope and map the threat events

C5. Identify and map the information assets impacted by each threat event

**Phase D: Vulnerability Assessment**

This step is unchanged.

D1. Identify vulnerabilities and related controls

D2. Assess the effectiveness of identified controls

D3. Determine the control strength for each combination of threat event and component
Phase E: Risk Evaluation

This phase is changed from the original IRAM2 setup. In this phase, I have added the CBA calculations. I have chosen to add them in this phase because the output of the previous phases (mostly step D but also the other previous phases) are needed for the CBA calculations to be correct and not be based on a qualified guess. The vulnerability for a specific risk is used to set a vulnerability level in CBA. The result from CBA is also needed in the next phase which is why it needs to be done before. The result from CBA will tell whether the security controls to choose from are economically effective or not. The result of the CBA is valuable decision support that helps in choosing risk treatment plan for each risk.

The steps are:
E1. Derive the likelihood of success
E2. Derive the residual likelihood
E3. Determine the residual business impact rating
E4. Derive the residual risk rating
E5. Calculate CBA (input from step previous steps)

Phase F: Risk Treatment

The steps in this phase are mostly remaining unchanged. The only change is that when choosing risk treatment for each risk, we now have information to help us make a more qualified decision. Thanks to the CBA, we now which treatments/security controls that are economically feasible and therefore we can choose the risk treatment that is most effective from both a security and economic perspective.

The steps of the final phase are:
F1. Evaluate each risk against the risk appetite
F2. Create a risk treatment plan (input from CBA)
F3. Execute the risk treatment plan and validate results
Design principles

As a result of this study, some design principles will be created that can be used in risk assessments that require financial indicators.

1. The work should start with conducting a traditional risk assessment method that suits the organization. When the risks are identified and the security measures that can be used to mitigate those risks are decided upon, that is when CBA should be conducted. In IRAM2 this is in relation to phase E and F, but most risk assessment methods have corresponding steps.

2. More traditional methods such as IRAM2 or others can be used as indications on what values to put in for some variables in CBA such as threat probability and vulnerability. Traditional risk assessments identify those values which are needed as input in CBA. If this is conducted, there is a systematic way to identify those values instead of best guesses based on how much organizational knowledge the assessor has.

3. Going through the risks that need to be mitigated and choosing the security measure that should be used to mitigate that risk should be done iteratively. This is where CBA is most valuable and helps with conducting the traditional risk assessment. CBA provides the financial aspect that is an important part of choosing the best security measure.

4. Combining traditional risk management (IRAM2 or other similar method) with financial risk management can provide results that are valuable for decision making. The financial effectiveness of a security investment is essential information when communicating with decision makers and trying to convince them regarding certain investments. The result of the CBA is used as decision support and support for communication with management.

ADR implementation

ADR has been implemented through following the steps that are suggested in the method and creating the hybrid method for combining traditional risk management with economic equations. Besides creating the method, more generalized design principles have been created. They can be used with other methods than the ones suggested in this study which makes them more usable and general. The work has been an iterative process and the design principles have
been revised throughout the work and adjusted based on the lessons that have been learned from implementing the methods.

The coat hanger model which is also an iterative process has been used to meet the evaluation criteria of ADR while still working in an iterative manner. Based on the ADR method, a clear problem was formulated based that needed intervention to be solved. The intervention was when the methods were implemented and tested in the organization to try and solve both a practical and a theoretical problem.

The building part of ADR was the process of creating the hybrid method and the design principles. The hybrid method is based on IRAM2 and CBA which have both been changed in the building process through implementing, reviewing, evaluating and then drawing conclusions about if there is any way to improve them. They have also been connected with each other to result in one cohesive method.

Reflecting and learning has been done throughout the process both individually and by interviewing stakeholders. I have received help with implementing IRAM2 and CBA and received input during the implementation process about how they perceive the method and if they see any problems with it. The reflections and input from stakeholders have been a big part in creating the design principles. The design principles are an attempt at generalizing the knowledge gained through the study and providing a result that can be used regardless of choice of method.

**Discussion and conclusion**

This is the chapter where the result is evaluated and discussed. There will also be conclusions drawn based on the implementation process, theory study and interviews.

**Evaluating methods**

In this section, the methods will be evaluated through own reflections based on implementation and interviews with stakeholders.
Discussion

IRAM2 is a relatively complex risk assessment methodology. The developers of the method promise simplicity and a practical approach to risk management. I would argue that there are simpler risk management approaches. In my opinion, the advantage of IRAM2 is not simplicity. The advantage is rather that it is very holistic from a security point of view and easy to use. It is clear what the meaning of each step is and how the phases relate to each other. It is a simple approach if we only compare it to complex risk management methods that include a lot of different aspects. There are other simpler approaches that don’t take as many aspects into consideration.

Getting valuable results from IRAM2 takes time and requires involvement from different parts of the organization. When including CBA and using the hybrid method, it adds an extra level of complexity. There has to be discussions within each organization to conclude if it is worth it to invest the time to get control over their risks and security investments. If it is worth it then there should be discussions on how and when to do the risk assessments. They can be done with a regular time interval or in combination with big projects or changes.

Essentially, the goal at SEB Kort is to get the risks under control and mitigate what needs to be mitigated. The security investments always need to be prioritized together with all the other activities in the organization. There are many projects and investments that compete regarding resources. This is one of the reasons that traditional risk management needs to be combined with CBA, so that the financial benefits of prioritizing the security measure that mitigates risk can be presented.

The other option is to choose which security measure to invest in solely based on the effectiveness of the security measure from a risk mitigating perspective. The previous studies show that economic incentives to invest in security measures becoming an increasingly essential part of mitigating risks. There is a challenge for security professionals to receive the resources and investments needed to mitigate the risks that they have identified. The previous studies and this study as well show that the financial aspects are a key to convincing management to invest.
Therefore, my conclusion is that solely focusing on effectiveness from a security perspective and not including a financial aspect is not sufficient.

I suggest that the modifications I did to the CBA method used is considered when doing CBA since in my opinion, equation 18 did not work to get a usable result. The value of the risk before and after the security measure became the same which it isn’t supposed to. The changes where to how ROI and benefits where calculated.

IRAM2 is a well-known and used widely in the information security industry. However, there are a lot of organizations that use other risk assessment methods with other advantages and disadvantages. The point of this study is not to widen the use of IRAM2 but to show that traditional risk management methods can be combined with CBA to get a better result. IRAM2 has been used as an example to portray that point. In traditional risk assessment in general, the vulnerabilities are assessed and the risks that need to be mitigated are identified. The final step in general is to create a risk treatment plan and decide what security measures to invest in if any. Other options can be to leave things as they are, transfer or outsource risk etc. In any case that a security measure is to be chosen to invest in, CBA can be used to identify which ones are economically feasible to invest in. This provides valuable input when it comes to choosing security measure. It is also valuable information that can be used to convince management to invest in the chosen security measures.

**Interviews**

Two interviews have been conducted for the evaluation. The CISO and IT manager at SEB Kort have been interviewed to evaluate how helpful the implementation of the hybrid method has been for them and their organization. The CISO has been involved in the process and has also been the one requesting a risk assessment, therefore the questions asked will be different. The interviews have been recorded and transcribed but the originals will not be posted since some parts have been left out for security reasons.
CISO

The CISO had been involved in some of the phases in the risk assessment and has been the one requesting a risk assessment for the specific project. He has also wanted help to introduce IRAM2 in SEB Kort and to implement it. He asked for an implementation in the specific project to test and see how it worked and how IRAM2 can be used in the organization. In the interview, I asked how the implementation went and if he thinks that this can be useful for SEB Kort in the future. I also asked in what way this risk assessment has benefited him and the risk management at SEB Kort. The CBA method will also be evaluated in the interview.

The CISO thinks that it is very good that we have done an extensive risk assessment which is something he wants more focus on. He felt that IRAM2 was suitable for our organization and our purposes which he has stated since before the implementation. He did feel that there were some steps that where unnecessary for doing a risk assessment on a project. The environmental perspectives are dealt with by other groups and in other forums. He had pointed this out early in the process and thereafter, those aspects were removed.

The CISO wants IRAM2 to become the standard risk assessment method used in this organization. He wants it to be used in every new project before it is released in production. He also wants our internal applications to be assessed through IRAM2 yearly. He stated that for bigger project (projects resulting in big changes in our applications or processes) he would like CBA to be used as a routine. Performing those tasks should be the responsibility of the information security department. However he does point out that this will be difficult from a resource perspective and that is the reason that it only should be done in relation to big changes. He thinks that the results from the CBA are useful but that it should only be used when there is a possibility to make an investment. Those situations can be when we find very high risks that need to be mitigated or when there is a big project that has a lot of financial resources allocated. In those situations, CBA can be used to choose what security measure to invest in and to provide concrete economic information to the decision makers so that they can make a qualified decision and see the economic benefits of their security investments.
He is the one that argues for the security investments at SEB Kort and has to convince management to invest in the security measure that he proposes. He states that it is valuable to be able to show the financial incentives of the investments. That management can see clearer that there is a financial gain in the proposed investments. However, he does think that the CBA is time consuming if it isn’t done in an automated tool and wishes that such tool can be used if one is invented instead of using resources to do the calculations. The result is useful and in some cases even necessary but there is some problems with reaching that result if there is a lack of resources or lack of knowledge in mathematical equations.

**IT manager**

The IT manager was not involved in requesting or implementing a risk assessment method. He thinks that those issues are important and wants risk assessment to be done continuously, but has delegated this to the information security department. He got involved after the implementation when it was time to discuss the results and what to mitigate. Mitigating risks is a financial issue and he is the one that needs to improve the costs and investments.

He thought that it made it a lot easier for him to make decisions when we could present the economic perspectives of the different security measures that could be used to mitigate our risks. It was easier for him to decide if it was an economically smart investment and if it is something he should prioritize or not. He was also pleased that he could see that it would not only be a cost but would also save him money in the long term. Even though this is something that we always try to communicate, he thought that it really went through for him when he could see the numbers and see that we actually had done the math.

There are both advantages and disadvantages with using a hybrid model between IRAM2 and CBA. The clear advantage is that it takes more time since it is both the traditional and the economic aspects need to be considered. The economic equations need to be done by someone who has knowledge of the costs and incomes of the organization, and preferably knowledge in economics. Finding someone who has time to do these calculations can be difficult, and it makes it more difficult that the person would require skills and knowledge that not everyone has. The benefit is quite clear as well; adding CBA or other economic methods to IRAM2 or
any other traditional method gives more material that can help getting the desired decisions and investments from management.

It is always an advantage for security professionals to be able to provide economic arguments and not only speak from a security point of view. We need to be able to convince managers that the investments we want are good for the organization economically. With the material that is the result from IRAM2 and CBA we can show that it is a smart investment that they will benefit from. Management tends to think that it is mostly costs with security investments and have difficulties seeing the benefits, especially the financial benefits.

Every organization needs to at different points of time consider if it is worth putting the time and effort to do these extensive risk assessments. Even though they can be simplified a bit, it is still a bit of work. Some organizations might want to do it once a year, some might want to do it when they start with a new project, and some might never do it and so on. The point is that when there is a need to get good material and take a qualified and economically effective decision, it will require work. In those cases, this hybrid method fulfills those purposes and works well to provide that material and insight.

**Conclusion**

To relate back to the research questions:

*What would the benefits be from introducing CBA to a more traditional risk management method?*

The benefits are quite clear; the CBA adds an economic perspective to traditional risk management methods that lack those aspects. In our scenario, we as information security officers were able to get our IT manager to understand the benefits of taking action based on our risk assessment work. CBA gave us the ability to figure out what was the economically reasonable thing to do and also to communicate it to our managers. It wasn’t only our opinion anymore; we had done the math and had the result of CBA as evidence.

If information security officers want to have evidence to prove their point and wants something to help them convince management that their recommended investment is worth the cost, having counted the benefits in monetary terms helped. In our case, it was what our
management needed to know that they were making the right decision. Without this information, they had always been insecure in whether to invest or not. In their perspective, we as information security professionals always think that it is worth it because we think that it is the most important thing, but for them it has to be prioritized together with all other potential investments that other people think are more important. Being able to show the financial incentives of security investments can help security professionals argue their case.

The results show that it did benefit us to be able to have the combination of information that we got from using both traditional and economic risk management methods and the result is a contribution to both theory and practice. Theoretically, this shows that it can be valuable to combine security and economic aspects more when working with risk management and that the traditional methods might not be sufficient anymore since the concept needs to be understood by top management to get resources. That is where the economic calculations are a valuable tool.

Even though the method doesn’t solve all problems with choosing which security investment to choose, it is a helpful tool that can be used to make a more qualified decision. Besides using methods and equations, the knowledge of the professionals in the field is always essential to making good decisions. No method can provide 100% accurate results since no method can help foresee the future and predict which security measures will keep our organizations safe. They can however be helpful in making qualified best guesses and this method is an attempt at becoming a helpful tool for that purpose.

**How will a hybrid risk management method with IRAM 2 and CBA combined work in a financial Institution?**

In a financial institution, there are a lot of risk assessments being done for different purposes. Information security risk management needs to be separated from other risk management methods that focus on financial risks such as credit risks. Those risks that only apply to financial institutions have been left out of scope. However, even when conducting information security risk management, there are certain issues that are specific for financial institutions. The financial industry is under constant attack and is always being targeted by criminals. This sets
high requirements for us working with risk management and making sure that the risks are being mitigated.

Financial institutions are also subject to a lot of legal and regulatory demands. IRAM2 takes those legal aspects into consideration, which makes that specific method suitable for a financial institution. Since financial institutions are known to be targets and also have high demands in information security both by customers and legislators, tend to have a big focus on risk assessment and risk mitigation. Because of the high standards that financial institutions have to apply to, these types of extensive risk assessment methods are justified. Even though they require a bit of work to reach a useable result, for institutions that have focus on these issues it is necessary to live up to the standards.

The practical contribution is that the methods where tested in a financial institution that can be used as a representative for the big banks and financial institutions in Sweden. Even though it cannot be generalized completely and the conclusion cannot be drawn that this will work in all financial intuitions, it can still help organizations decide how to work with risk management and show them that this is a potential way of working that might suit them. This is a contribution to hopefully one of several attempts to add financial perspectives to traditional risk management methods and one piece of the puzzle when it comes to changing the attitude when it comes to security and seeing it strictly as a cost.

The design principles are also a contribution to the theoretical field of risk management. The principles are more general and can be used as guidance to how to think when combining a traditional risk management method with a method with a financial focus. The principles can be used with other risk management methods and are therefore more generalized.
References


